REMARKS

Applicants would like to thank the Examiner for finding our arguments persuasive in the Pre-Appeal Brief Request for Review, and for reopening prosecution.

The independent claims have been amended to more clearly define the present invention over the cited prior art references. In particular, the input stage receives an input data block that is X bits in length and a key data block comprising a plurality of sub-key data blocks. The input stage adds the X bits of the input data block with a first sub-key data block to generate a summed signal that is X bits in length, and then divides the summed signal into N first signals that are in parallel. Each first signal is n bits in length so that n * N = X. Support for the claim amendments may be found in paragraph 28, for example, and as illustrated in FIG. 2.

The claim amendments and arguments supporting patentability of the claims are provided below.

I. The Amended Claims

The present invention, as recited in amended independent Claim 1, for example, is directed to a cryptographic device comprising an input stage, and an intermediate stage connected to the input stage. The input stage receives an input data block that is X bits in length and a key data block comprising a plurality of sub-key data blocks. The input stage adds the X bits of the input data block with a first sub-key data block to generate a summed signal that is X bits in length, and then divides the summed signal into N first signals that are in

parallel. Each first signal is n bits in length so that n * N = X.

The intermediate stage comprises a plurality of substitution units operating in parallel, each substituting data within a respective first signal. A diffuser is connected to the plurality of substitution units for mixing data to generate a diffused signal. The diffuser comprises at least one shift register and at least one look-up table associated therewith. An output stage is connected to the intermediate stage for repetitively looping back the diffused signal to the input stage for combination with a next sub-key data block.

Amended independent Claim 10 is directed to a communication system comprising a key scheduler and a cryptographic device connected to the key scheduler, and has been amended similar to amended independent Claim 1.

Amended independent Claim 18 is directed to a method for converting an input data block into an output signal in a cryptographic device, and has been amended similar to amended independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 10 and 18 over the Kanda et al. patent in view of the Stein et al. published patent application. In Kanda et al., the Examiner characterized reference **17** in FIG. 2 as an input stage generating a plurality of first signals that are in parallel. The Examiner also characterized substitution units S_0-S_7 as part of the intermediate stage, wherein the substitution units operate in

parallel, with each one substituting data within a respective first signal.

In FIG. 5 of Kanda et al., the Examiner characterized block **346** as a diffuser connected to the plurality of substitution units S_0-S_7 for mixing data to generate a diffused signal. As correctly noted by the Examiner, the combining part **346** does not include a shift register and a look-up table for mixing data to generate a diffused signal. Instead, the combining part **346** merely combines the outputs from the non-linear transformation parts 345_0-345_3 without mixing the outputs therefrom.

In FIG. 4 of Kanda et al., the Examiner characterized the output stage as the round processing 38_0-38_{N-1}, where each processing part provides an output to the next one of the processing parts for combining with another subkey data block. The Examiner has characterized that the round processing 38_0-38_{N-1} corresponds to the repetitively looping back in the claimed invention.

The Examiner cited Stein et al. as disclosing a diffuser including a shift register and a look-up table for mixing data to generate a diffused signal. In particular, the Examiner referenced FIG. 2 and paragraphs 31 and 33 in Stein et al. FIG. 2 illustrates that data undergoes transformation in an S-Box **18** and then a shift row transformation **20** (which corresponds to a shift register) followed by a mix column transformation **22**.

The Examiner states that the combination of the shift

row transformation **20** and the mix column transformation **22** operations that are carried out after the S-Box transformation operation corresponds (or is functionally equivalent) to the diffuser as recited in the claimed invention. In paragraph 33 of Stein et al., the Examiner has taken the position that a parallel look-up table performs shift row transformation in addition to a parallel look-up table for S-box transformation. In other words, the Examiner is characterizing a shift row transformation and a mix column transformation as including a look-up table as corresponding to the diffuser in the claimed invention.

The Applicants submit that even if the references were selectively combined as suggested by the Examiner, the claimed invention is still not produced. First, the length of the input data in Kanda et al. is split into left and right portions L_0, R_0. Kanda et al. discloses that the intermediate stage (i.e., substitution units S_0-S_7 and diffuser **346**) only operates on the right portion R_0. As best illustrated in FIG. 4 in Kanda et al., the input data is 64 bits in length, and is divided in a left portion L_0 that is 32 bits in length and a right portion R_0 that is also 32 bits in length. The right portion R_0 is applied to the nonlinear function part **304**, which includes the intermediate stage as in the claimed invention. The left portion L_0 corresponds to the **XOR** circuit 12 in FIG. 1 and a swapping part **306**.

In sharp contrast, the claimed invention recites that the input stage receives an input data block that is X bits in length and a key data block comprising a plurality of sub-key

data blocks. The input stage adds the X bits of the input data block with a first sub-key data block to generate a summed signal that is X bits in length, and then divides the summed signal into N first signals that are in parallel. Each first signal is n bits in length so that n * N = X. Support for the claim amendments may be found in paragraph 28, for example, and as illustrated in FIG. 2. In other words, the input data is not split into left and right portions.

Secondly, in reference to paragraph 33 and FIG. 6 in Stein et al., a parallel look-up table **60** performs the S-Box transformation, a parallel look-up table **62** performs the shift row transformation, and a Galois field multiplier **64** performs the mix column and key addition operation. The Applicants submit that Stein et al. fails to disclose that the diffuser itself comprises at least one shift register and at least one look-up table associated therewith - as in the claimed invention. Even if look-up table **62** is considered part of the diffuser and corresponds to the shift register, the Galois field multiplier **64** is not a look-up table.

In reference to paragraph 31 and FIG. 2 in Stein et al., the data undergoes transformation in an S-Box **18** and then a shift row transformation **20** followed by a mix column transformation **22**. First, the Applicants submit that a mix column transformation **22** is not the same as a look-up table as recited in the claimed invention.

The Applicants submit that it would not have been obvious to modify the diffuser **346** in Kanda et al. as suggested

by the Examiner. Dependent Claim 4 in the claimed invention recites that the each substation unit performs a substitution based on a look-up table. The Applicants submit that modifying Kanda et al. to include a shift row transformation **20** and a mix column transformation **22** is more applicable to the substitution units S_0-S_7 disclosed therein as compared to the diffuser **346**. In addition, as best illustrated in FIG. 2 in the present application, the output stage **26** comprises a row shift **32** followed by a column mix **36** - the same as what is disclosed by Stein et al. The Applicants further submit that modifying Kanda et al. to include a shift row transformation **20** and a mix column transformation **22** is more applicable to the output stage disclosed therein as compared to the diffuser **346**.

The diffuser in the claimed invention adds computational complexity for enhancing the cryptography. The diffuser comprises a shift register **60** and a look-up table **62** as illustrated in FIG. 4 to advantageously provide a minimum number of cycles that the diffuser circulates to provide bit-wise mixing across the entire shift register. This is not possible with the shift row transformation **20** followed by the mix column transformation **22** as disclosed in Stein et al.

Accordingly, it is submitted that amended independent Claim 1 is patentable over Kanda et al. in view of Stein et al. Amended independent Claims 10 and 18 are similar to amended independent Claim 1. Therefore, it is submitted that these claims are also patentable over Kanda et al. in view of Stein et al.

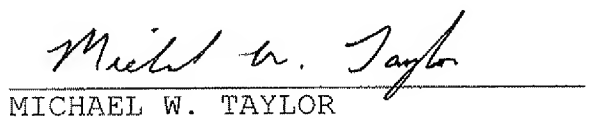
In view of the patentability of amended independent

Claims 1, 10 and 18, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the claim amendments and arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330